

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
Université des Sciences et de la Technologie Houari Boumediene**



**Faculté d'Electrique - Informatique**  
Département d'informatique



Mémoire de Fin d'Etude pour l'obtention du diplôme  
d'Ingénieur d'Etat en Informatique.

Option : Software

**Thème :**

**Un outil automatique intelligent d'aide à  
la prise de décisions dans  
Firewall Forensics**

Organisme d'accueil : **C.E.R.I.S.T.**

Thème Proposé et Encadré par :

**Mme H.Aliane**

**M<sup>elle</sup> H.Bensefia**

Présenté par :

**Mr Benrejdal Samir**

**Mr Korichi Houari**

Soutenu devant le jury :

**Mr Benabadji** Président du jury

**Mr Laichi** Membre du jury

**Mr Bouabana** Membre du jury

**PROMOTION : 2004 / N°65**

# TABLE DES MATIERES

<b>INTRODUCTION GENERALE.....</b>	<b>1</b>
<b>I. LE MODELE TCP/IP :.....</b>	<b>3</b>
1. Introduction :.....	3
2. Présentation de TCP/IP :.....	4
2.1. Définition :.....	4
2.2. L'adressage :.....	4
2.2.1. Adresse physique:.....	4
2.2.2. Adresses IP:.....	4
- les classes d'adresses IP :.....	4
2.3 .Architecture des protocoles TCP/IP :.....	6
2.3.1. La couche physique :.....	7
a - Le Protocole ARP :.....	7
b- Le Protocole RARP :.....	7
2.3.2. La couche Internet(IP) :.....	7
a- Le Protocole IP :.....	8
- Les Datagrammes :.....	8
b- Le Protocole ICMP :.....	9
2.3.3. La couche Transport(TCP) :.....	9
a- Le protocole UDP :.....	9
- Les Ports :.....	10
- Les ports réservés :.....	10
- Les ports enregistrés :.....	10
- Les ports dynamiquement alloués :.....	10
- Format d'un paquet UDP :.....	10
b- Le protocole TCP :.....	11
- Format d'un segment TCP :.....	12
- L'établissement d'une connexion :.....	13
2.3.4. La couche application :.....	14
3.Conclusion :.....	14
<b>II. LES FIREWALLS.....</b>	<b>15</b>
1. Introduction :.....	15
2. Définitions d'un firewall :.....	15
3. L'emplacement d'un firewall :.....	15
4. Les principales classes de firewall :.....	16
4.1. Firewall software :.....	16
4.2. Firewall hardware :.....	16
5. Le rôle du firewall :.....	16
6. La politique de sécurité du réseau :.....	16
6.1. Politique d'accès aux services réseau :.....	17
6.2. La politique de conception du firewall :.....	17
7. Les technologies des firewalls :.....	17
7.1. Les filtres à paquet :.....	17

<i>Définition</i> :	17
<i>Les avantages de filtres à paquet</i> :	18
<i>Les Limites de filtres à paquet</i> :	18
7.2. <i>Les passerelles d'application</i> :	18
<i>Définition</i> :	18
<i>Les avantages des passerelles d'application</i> :	18
<i>Les Limites des passerelles d'application</i> :	19
7.3. <i>Les firewalls à inspection de paquets</i> :	19
<i>Définition</i> :	19
<i>Les avantages des firewalls à inspection de paquets</i> :	19
<i>Les limites des firewalls à inspection de paquets</i> :	19
8. Les principales Architectures de firewall :	19
8.1. <i>Architecture d'hôte à double réseau</i> :	20
<i>Définition</i> :	20
<i>Les avantages de l'architecture d'hôte à double réseau</i> :	20
<i>Les limites de l'architecture d'hôte à double réseau</i> :	20
8.2. <i>Architecture d'hôte à écran</i> :	20
<i>Définition</i> :	20
<i>Les avantages de l'architecture d'hôte à écran</i> :	21
<i>Les limites de l'architecture d'hôte à écran</i> :	21
8.3. <i>Architecture de sous réseau filtré</i> :	21
<i>Définition</i> :	21
<i>Les avantages de l'architecture de sous réseau privé</i> :	22
<i>Les limites de l'architecture de sous réseau privé</i> :	22
9. La journalisation dans les firewalls:	22
10. Les avantages du firewall :	22
11. Les limites du firewall :	22
12. Conclusion :	22
<b>III. NETWORK FORENSICS.....</b>	<b>23</b>
1. Introduction :	23
2. Les conséquences des attaques sur les organisations :	24
3. Traitement des attaques :	24
4. La réponse aux attaques :	24
- <i>Reprendre la production</i> :	25
- <i>Demande l'exécution d'une investigation</i> :	25
5. Forensics:	25
5.1. <i>Définition de Forensics</i> :	25
5.2. <i>Le besoin de Forensics dans la sécurité informatique</i> :	25
6. Computer Forensics :	25
6.1. <i>Définition</i> :	25
6.2. <i>La preuve informatique</i> :	25
6.2.1. <i>Définition</i> :	25
6.2.2. <i>Les catégories de la preuve:</i>	26
- <i>hardware</i> :	26
- <i>Software</i> :	26
6.2.3. <i>L'emplacement de la preuve:</i>	26
6.2.4. <i>La source de la preuve:</i>	26
7. Network Forensics :	26
8. Les étapes du processus de Network Forensics :	26

8.1. La préparation :	27
8.2. La collection :	27
8.3. L'identification :	27
8.4. L'investigation :	27
8.4.1. La phase de conservation :	28
8.4.2. La phase d'Examination :	28
8.4.3. La phase d'analyse :	28
8.4.4. La phase de présentation :	28
8.5. La notation :	28
9. Exemple d'investigation réel :	29
10. Conclusion :	29
<b>IV. LES FICHIERS LOGS :</b>	<b>30</b>
1. Introduction :	30
2. Définitions d'un fichier log :	31
3. Domaine d'utilisation des fichiers logs :	31
4. Les fichiers logs d'un firewall :	31
5. Le format de fichier log d'un firewall :	31
6. Périodes de génération de fichier log :	33
7. Les problèmes liés aux fichiers logs :	33
8. La protection des fichiers logs :	33
8.1. L'activation de l'opération d'enregistrement :	33
8.2. Mettre des autorisations adéquates :	33
8.3. Utilisation d'un serveur séparé :	33
8.4. Le cryptage :	34
8.5. Ecriture une fois :	34
9. La rotation des fichiers logs :	34
10. L'interprétation des fichiers logs :	34
11. Conclusion :	34
<b>V. LES SYSTEMES MULTI AGENTS :</b>	<b>35</b>
1. Introduction :	35
2. Les agents :	35
2.1. Définition d'un agent :	35
2.2. Déterminant d'un agent :	36
2.3. Caractéristiques d'un agent :	36
2.3.1. Autonomie :	36
2.3.2. Rationalité :	36
2.3.3. Intelligence :	36
2.3.4. Intentionnalité :	36
2.3.5. Adaptabilité :	36
2.4. L'environnement d'un agent :	36
2.5. Les modules d'un agent intelligent :	37
2.6. Modèles d'agents :	37
2.6.1. Agent réactif :	37
2.6.2. Agent cognitif :	38
2.7. Fonctionnement d'un agent :	39
3. Les Système Multi Agent (SMA) :	39
3.1. Définition d'un SMA :	39
3.2. Caractéristiques d'un SMA :	40

3.2.1. <i>Coordination et coopération</i> :	40
3.2.2. <i>Cohérence</i> :	40
3.2.3. <i>Contrôle</i> :	40
3.2.4. <i>Négociation</i> :	41
3.3. <i>Modèle de SMA</i> :	41
3.3.1. <i>Les Système à tableaux noirs</i> :	41
3.3.2. <i>Le modèle acteur</i> :	41
3.4. <i>L'organisation des agents</i> :	42
3.4.1. <i>Organisation centralisé</i> :	42
3.4.2. <i>Organisation libre</i> :	42
3.5. <i>Modèle de communication</i> :	42
3.5.1. <i>Communication par l'envoi des messages</i> :	42
3.5.2. <i>Communication par partage l'information</i> :	43
3.5.3. <i>La politique de communication</i> :	43
3.5.4. <i>Les langages de communication</i> :	43
4. <i>Conclusion</i> :	43
<b>VI. LA CONCEPTION ET MODELISATION.....</b>	<b>44</b>
1. <i>Introduction</i> :	44
2. <i>Le Firewall Forensics</i> :	44
3. <i>Les fichiers logs d'un firewall</i> :	45
4. <i>Réponse à la problématique</i> :	45
5. <i>Approche &amp; méthodologie</i> :	46
5.1. <i>Le format du fichier log d'un firewall</i> :	48
5.1.1. <i>La rotation du fichier log</i> :	48
5.2. <i>Le collecteur</i> :	48
5.2.1. <i>La session d'activités</i> :	49
5.2.2. <i>La table de translation</i> :	49
5.2.3. <i>Les connaissances du collecteur</i> :	49
5.2.4. <i>L'environnement du collecteur</i> :	49
5.2.5. <i>Le raisonnement du collecteur</i> :	49
5.3. <i>La base des activités</i> :	50
5.3.1. <i>Format</i> :	51
5.3.2. <i>La Rotation de la base des activités</i> :	51
5.4. <i>L'inspecteur</i> :	51
5.4.1. <i>Les connaissance de l'inspecteur</i> :	52
5.4.1.1. <i>L'ensemble des activités malicieuses prédéfinies</i> :	52
5.4.1.2. <i>La table des sessions malicieuses</i> :	52
5.4.2. <i>L'environnement de l'inspecteur</i> :	52
5.4.3. <i>Le raisonnement de l'inspecteur</i> :	52
5.5. <i>L'investigateur</i> :	53
5.5.1. <i>Les connaissances de l'investigateur</i> :	53
5.5.2. <i>L'environnement de l'investigateur</i> :	54
5.5.3. <i>Le raisonnement de l'investigateur</i> :	54
5.5.3.1. <i>Le raisonnement de l'investigateur pour l'activité</i> :	54
5.5.3.2. <i>Le raisonnement de l'investigateur pour la session</i> :	55
5.5.4. <i>Le format d'un rapport</i> :	55
5.6. <i>La base des archives</i> :	56
5.7. <i>La communication entre les agents et le modèle Multi-agents adopté</i> :	56
5.7.1. <i>La communication entre le collecteur et l'inspecteur</i> :	56

5.7.2. <i>La communication entre l'inspecteur et l'investigateur</i> :.....	57
5.8. <i>Interface utilisateur -système:</i> .....	57
5.9. <i>Interface expert –système</i> :.....	57
6. Modélisation :.....	59
6.1. <i>Diagramme de classes</i> :.....	59
6.2. <i>Diagramme de séquences</i> :.....	61
6.3. <i>Diagramme d'activités</i> :.....	62
7. Conclusion :.....	63
<b>VII. IMPLEMENTATION.....</b>	<b>64</b>
1. Introduction :.....	64
2. Le langage de développement :.....	64
3. Le langage de programmation JAVA :.....	64
4. Les éléments de base utilisés dans l'implémentation :.....	64
4.1. <i>Les Threads</i> :.....	65
4.2. <i>Les Vecteurs</i> :.....	65
4.3. <i>Les Fichiers</i> :.....	65
5. L'implémentation du Collecteur :.....	65
5.1. <i>L'implémentation de la table de translation</i> :.....	65
6. L'implémentation de la base des activités :.....	65
7. L'implémentation de l'inspecteur :.....	66
7.1. <i>L'implémentation de la table des activités malicieuses prédéfinies</i> :.....	66
7.2. <i>L'implémentation de la table des sessions malicieuses</i> :.....	66
8. L'implémentation de investigateur :.....	66
8.1. <i>L'implémentation de la base de connaissances</i> :.....	66
8.2. <i>L'implémentation de l'archive</i> :.....	66
9. l'implémentation de l'interface système - expert :.....	66
9.1. <i>Ajouter une activité malicieuse</i> :.....	67
9.2. <i>Ajouter une explication</i> :.....	67
10. l'implémentation de l'interface système –utilisateur :.....	67
10.1. <i>Rechercher une explication</i> :.....	68
10.2. <i>Voir l'archive</i> :.....	68
11. Les messages d'alerte :.....	68
12. Conclusion :.....	69
<b>CONCLUSION GENERALE .....</b>	<b>70</b>
<b>ANNEXE A : LES ACTIVITES MALICIEUSES PREDIFINIES.....</b>	<b>71</b>
<b>ANNEXE B : LA BASE DE CONNAISSANCES.....</b>	<b>74</b>
<b>ANNEXE C : Le langage UML .....</b>	<b>80</b>
<b>BIBLIOGRAPHIE.....</b>	<b>82</b>